1.0 INFORMATION ASSURANCE BACKGROUND

OMB Circular A-130, "Management of Federal Information Resources," requires Certification and Accreditation (C&A) of all federal Automated Information Systems (AISs)/networks every three years at a minimum or as changes that require re-accreditation occur. Further, the accrediting agency may request annual systems reviews. This C&A requirement ensures the effective safeguarding of sensitive but unclassified (SBU) information against unauthorized modification, disclosure, destruction, and denial of service.

Certification is the comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system. Certification is conducted in support of the accreditation process, to establish the extent that a particular system design and implementation meet a set of specified security requirements. Certification also determines the appropriate level of protection for the AIS/network. Accreditation is the formal approval by the Government to:

- Operate the AIS/network in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
- Operate within the given operational environment with stated interconnections.
- Operate with appropriate level-of-protection for the specified period.

The Military Health System (MHS) performs C&A of its AISs/networks in accordance with DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," as stipulated by OMB Circular A-130. The objective of the DITSCAP is to maintain a standardized approach to security C&A for AISs and communication networks. The process is designed to protect and secure those entities that comprise the Global Information Grid (GIG). The process is comprehensive and considers the AIS/network mission, environment, and architecture while assessing the impact of operation of that AIS/network on the GIG. One key aspect the C&A process checks is whether appropriate actions have been initiated to ensure compliance with DoD 5200.2-R, "Personnel Security Program," which requires all contractors who manage, design, develop, operate or access DoD AISs/networks or process MHS SBU information, to undergo an appropriate background investigation and security awareness training before access is granted to a DoD AIS/network or MHS SBU information.

Adherence to these requirements provides protection of DoD AISs/networks and MHS SBU information and is an absolute priority in order to provide world-class health support to the warfighter during peacetime and wartime.

2.0 TECHNICAL SERVICES REQUIRED

2.1 INFORMATION ASSURANCE TASK DESCRIPTION

The contractor shall ensure DITSCAP documentation availability and MHS acceptability, assist the government's MHS Information Assurance (IA) C&A Team during all phases of the C&A process, implement processes to provide a C2 level of security for MHS SBU information, and ensure appropriate background investigations are initiated and security awareness training for their personnel is completed before access to DoD AISs/networks or MHS SBU information is granted. The contractor shall coordinate all activities associated with this task, with the MHS IA

Program Office, the Contracting Officer's Technical Representative, and the DITSCAP Designated Approving Authority (DAA) when appropriate, before any action is taken.

2.2 SCOPE OF WORK

The C&A and Automated Data Processing/Information Technology (ADP/IT) background investigation requirements apply to contractors that manage, design, develop, operate, or access DoD AISs/networks and MHS SBU information. Government Owned Contractor Operated (GOCO) and Contractor Owned Contractor Operated (COCO) AISs/networks that process MHS SBU information are also bound by these requirements. The only exception is when the COCO AIS/network does not have connectivity with a DoD AIS or network. In this case the DITSCAP requirements do not apply, and other safeguards may be used in lieu of background checks for the investigation process, such as non-disclosure agreements and appropriate training. When completing the DITSCAP investigation, the contractor shall prepare all required documents and modify those documents as necessary to incorporate any Certification Authority (CA) recommendations. Contractor shall be required to mitigate vulnerabilities identified during the risk assessment process. The contractor shall work with the MHS IA C&A Team during the DITSCAP by providing technical (systems security) information and AIS/network access as needed to thoroughly execute the C&A mission. In addition, the contractor shall implement organizational processes necessary to provide a Trusted Computing Security Evaluation Criteria (TCSEC) C2 level of security for MHS SBU information. Furthermore, the contractor shall prepare, submit, and maintain copies of all required documentation to initiate the investigative process and validate any ADP/IT background investigation requirements. Finally, all C&A and ADP/IT background investigation activities must be coordinated with the MHS IA Program Office, the Contracting Officer's Technical Representative, and the DITSCAP DAA as appropriate.

2.3 STATEMENT OF WORK

The contractor shall acquire/develop and maintain DITSCAP documentation to ensure both initial and continued DITSCAP compliance for all contractor AISs/networks processing MHS SBU information. In addition, the contractor shall modify the DITSCAP documents as required to address system and/or procedural changes. The contractor shall assist the MHS IA C&A Team during all phases of the C&A process by providing documentation in accordance with the MHS IA C&A schedule. Upon contract award, the contractor must be prepared to execute the DITSCAP process by providing required documentation necessary to receive an Approval to Operate (ATO), and by making the contractor's AIS(s)/networks available for testing. Contractor will be required to mitigate vulnerabilities identified during the risk assessment process. These requirements must be met before fielding the system, and before connectivity to any DoD AIS or network is authorized. The only exception is when the COCO AIS/network does not have connectivity with a DoD AIS or network, when DITSCAP requirements do not apply. However, the contractor shall put in place processes that provide and ensure security protection for any GOCO and/or COCO AISs/networks that process MHS SBU information. When required, the contractor shall initiate and document all activities necessary to establish any ADP/IT background investigations for each contractor employee required to support the ADP/IT level of the positions held. This ADP/IT process establishes the level of access to be afforded to

every contractor employee using DoD AISs and networks, as well as individuals accessing MHS SBU information.

2.3.1 DITSCAP Documentation

The contractor shall provide all necessary DITSCAP documentation and take all necessary steps to achieve accreditation. During the period of performance, the contractor shall modify DITSCAP documents to incorporate the comments of the CA and/or to account for system changes made to the contractor AISs/networks processing MHS SBU information. All AISs and networks that process, sort, transmit, or access sensitive MHS SBU information (including patient medical data) shall require security C&A in accordance with DoD DITSCAP (DoDI 5200.40).

The contractor shall produce and finalize all DITSCAP documents for contractor AISs/networks processing MHS SBU information, including preparation of a System Security Authorization Agreement (SSAA) and required appendices (Deliverable #1). The SSAA is the defining document that supports the DITSCAP. The SSAA is a living document that is used throughout the entire DITSCAP to guide actions, document decisions, specify Information Technology Security Evaluation Criteria (ITSEC) requirements, identify potential solutions to risks and vulnerabilities identified, and maintain operational security. The primary objectives of the SSAA are to document:

- The formal written agreement among the DAA, CA, User Representative, and Program Manager.
- All requirements necessary for accreditation and how requirements are met.
- All security criteria required throughout the AIS/network life cycle.
- The DITSCAP Plan (e.g., a list of activities and associated timelines for achieving C&A).

The SSAA consolidates the system and security documentation into one master document. This eliminates redundancy and potential confusion. When feasible, the SSAA can be tailored to incorporate existing documents as appendices or by reference to the pertinent document.

The required core chapters within the body of the SSAA shall include the following:

- Chapter 1 - Mission Description and System Identification
- Chapter 2 - Environment Description
- Chapter 3 - System Architectural Description
- Chapter 4 - System Security Requirements
- Chapter 5 - Organizations and Resources
- Chapter 6 - DITSCAP Plan

Additionally, the contractor shall provide the following documents as SSAA appendices:

- Acronym List
- Glossary of Terms
- Reference List
- System Concept of Operations

- Information System Security Policy
- Requirements Traceability Matrix
- Certification Test and Evaluation Plan
- Security Test and Evaluation (ST&E) Procedures
- Security Features Users Guide (SFUG)
- Trusted Facility Manual (TFM)
- Security Design Document (SDD)
- Configuration Management Plan
- Installation Guide
- Rules of Behavior
- Incident Response Plan
- Contingency Plans
- Personnel and Technical Security Controls
- MOA's for System Interfaces
- Security Awareness Training Program

2.3.2 MHS IA C&A Team

The contractor shall assist the government's MHS IA C&A Team during all phases of the DITSCAP. The MHS IA C&A Team shall require systems access in order to facilitate the script testing and automated scanning necessary to qualify the contractor's AISs/networks for C&A. All scans and testing shall be scheduled and conducted in coordination with the MHS IA Program Office, the Contractor, and the Contracting Officer's Technical Representative.

2.3.3 TCSEC C2 Level Processes

The MHS IA Program Office requires all contractors who manage, design, develop, operate, or access DoD AISs/networks or process MHS SBU information to ensure that an appropriate and consistent level of security is achieved. In order to protect and maintain availability, integrity, authentication, confidentiality, and non-repudiation of MHS SBU information, TCSEC C2 protection is mandatory. The only exception is when the COCO AIS/network does not have connectivity with a DoD AIS or network, when TCSEC C2 requirements do not apply. These requirements are defined in the DoD 5200.28-STD. Therefore, the contractor must:

- Ensure that their personnel receive initial and annual IA training before accessing DoD AISs/networks, and MHS SBU information.
- Protect all contractor AISs/networks and equipment that process MHS SBU information at a level that is equal to, or greater than, the highest level of security protection for any information processed, stored, transmitted, or accessed.
- Implement network security measures to prevent unauthorized access.

- Obtain security (DITSCAP) C&A documents published by DoD for all AISs/networks that process, store, transmit, or access MHS SBU information, if the AIS/Network connects to a DoD system.
- Comply with the requirements for Information Assurance Vulnerability Alert (IAVA) in accordance with the Office of the Deputy Secretary of Defense Policy Memorandum, DoD Information Assurance Vulnerability Alert. Contractors can sign-up to a List Server for IAVA notifications at www.cert.mil or www.cert.org.
- Report out-of-the-ordinary events such as intrusion, denials of service, malicious logic attacks, and probes to a Computer Emergency Response Team (CERT). MHS Contractor sites should have a structured ability to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of operations. These incidents must be reported to the CERT immediately.

2.3.4 ADP/IT Requirements

The MHS IA Program Office, in compliance with DoD 5200.2-R - Personnel Security Program, January 1987, requires all contractors who manage, design, develop, operate or access DoD AIS or network to process an appropriate background investigation and security awareness training before access is granted to an AIS or network. The only exception is when a COCO AIS/network does not have connectivity with a DoD AIS or network. In this case, background investigations for contractor personnel are not required and other safeguards may be used, such as non-disclosure agreements and appropriate security training. A level of trustworthiness must be established before granting access to MHS SBU information. Therefore, the contractor must:

- Initiate, maintain, and document minimum personnel security investigations appropriate to the individual's responsibilities and access to MHS SBU information.
- Immediately report to the appropriate government representative if any contractor employee filling a sensitive position receives an unfavorable National Agency Check (NAC) adjudication, or if information that would result in an unfavorable NAC becomes known.
- Immediately deny access to any AIS, network or MHS SBU information to any contractor employee if, at any time, the individual receives an unfavorable NAC adjudication, or if directed to do so by the appropriate government representative for security reasons.
- Ensure all contractor personnel receive IA training before being granted access to DoD AISs/networks, and/or MHS SBU information.

All contractor personnel must be designated as ADP/IT-I, ADP/IT-II, or ADP/IT-III where their duties meet the criteria of these position sensitivity designations as described in Appendix K, DoD 5200.2-R. Investigations appropriate for position sensitivity designations are (see Paragraph 3-614, DoD 5200.2-R).

ADP/IT I Background Investigation (BI)

ADP/IT II DoD National Agency Check Plus Written Inquiries (DNACI) or National Agency Check Plus Written Inquiries (NACI)

ADP/IT III National Agency Check (NAC) or Entrance National Agency Check (ENTNAC).

Interim Assignment: Individuals, except non-U.S. citizens, to include temporary, intermittent and seasonal personnel, efforts will be taken to approve ADP/IT-I, ADP/IT-II, and ADP/IT-III positions on an interim basis prior to a final adjudication of the required personnel security investigation only after the conditions specified below have been met.

ADP/IT-I:

- Favorable completion of the NAC
- Initiation of an SF85P and Supplemental Questionnaire (when required)

ADP/IT-II:

- A favorable review of local personnel, base/military, medical, and other security records as appropriate
- Initiation of a NACI, as appropriate/favorable review and submission of SF85P and Supplemental Questionnaire (when required)

ADP/IT-III:

- A favorable review of local personnel, base/military, medical, and other security records as appropriate
- Initiation of a NAC, as appropriate/favorable review and submission of SF85P and Supplemental Questionnaire (when required)

For DoD contractor personnel, any interim approval shall be made by the government sponsor's security manager/official.

2.3.4.1 ADP/IT Positions Categories

In establishing the categories of positions, other factors may affect the determination, permitting placement in higher or lower categories based on the agency's judgment as to the unique characteristics of the system or the safeguards protecting the system. A level of trustworthiness must be established before granting personnel access to MHS SBU information, DoD AISs/networks or contractor AISs/networks with DoD connectivity, to include:

- ADP/IT-1 Critical Sensitive Position. Those positions in which the individual is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or

maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

- ADP/IT-II Noncritical-Sensitive Position. Those positions in which the individual is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP/IT-I category to insure the integrity of the system.
- ADP/IT-III Nonsensitive Position. All other positions involved in computer activities.

Each contractor shall be required to complete and submit for appropriate personnel the Standard Form 85-P, "Questionnaire for Public Trust Positions," fingerprint forms, and such other documentation as may be required by the Office of Personnel Management (OPM) to open and complete investigations. Following submission, an interim (temporary) clearance may be provided while this investigation is ongoing. Forms and guidance can be found at www.opm.gov/extra/investigate

2.3.4.2 Non-U.S. Citizens

Non-U.S. citizen contractor employees shall not be assigned to ADP/IT-I positions.

Non-U.S. citizen contractor employees assigned to ADP/IT-II or ADP/IT-III positions must have a completed investigation and favorable adjudication prior to access.

Interim access is not authorized.